

Security improvement of using modified coherent state for quantum cryptography

Y. J. Lu,^{*} Luobei Zhu,[†] and Z. Y. Ou[‡]

*Department of Physics,
Indiana University-Purdue University Indianapolis
402 N Blackford Street, Indianapolis, In 46202*

(Dated: February 1, 2008)

Weak coherent states as a photon source for quantum cryptography have limit in secure data rate and transmission distance because of the presence of multi-photon events and loss in transmission line. Two-photon events in a coherent state can be taken out by a two-photon interference scheme. We investigate the security issue of utilizing this modified coherent state in quantum cryptography. A 4 dB improvement in secure data rate or a nearly two-fold increase in transmission distance over the coherent state are found. With a recently proposed and improved encoding strategy, further improvement is possible.

PACS numbers: PACS Number: 03.67.Dd, 42.50.Dv, 42.50.Ar

I. INTRODUCTION

The ultimate security of quantum cryptography stems from the non-cloning theorem[1] of quantum mechanics, which is applied to a single quantum system. In other words, quantum information can only be shared between two parties, the one (Alice) who creates it and the one (Bob) who receives it. Therefore, in the implementation in optical communication, the ideal source is a single photon source with information carried by individual photons. So far a weak coherent state from a laser is closest to a single photon source for quantum cryptography. The experimental realization[2] of the first proposed quantum cryptography protocol, known as BB84 protocol[3], involved a heavily attenuated thermal source (which is worse than a laser in the aspect of multi-photon events). However, the existence of multiple photon events for a weak coherent state, even though very rare, poses serious problem for the security of the protocol. An eavesdropper (Eve) can in principle use the so-called photon number splitting attack to tap the information without being noticed. Recent analysis by Lütkenhaus[4] on the security of quantum cryptography by a weak coherent state puts limit on the data rate and transmission distance for secure key distribution.

Significant progress has been made in producing single photon states[5, 6, 7, 8, 9, 10, 11, 12, 13]. But so far these sources are fluorescence-based and have small efficiency. Furthermore, because the emission depends on energy structure, it has a fixed wavelength and a finite time response for high repetition rate. So they are limited for practical applications. Recently a new scheme was proposed[14] and realized[15] for producing a photon source with same single photon rate as a coherent state but less two-photon events. The scheme relies on

a two-photon quantum interference phenomenon to reduce and eventually cancel the two-photon events from a coherent state. Although it cannot take out all the multi-photon events, it does take out the most dominating multi-photon events – two-photon events. This modified coherent state (MCS) has the advantages of high data rate, well defined direction and wave-length independence for practical application in quantum cryptography.

A new quantum cryptography protocol(SARG04) was recently proposed[16] against the photon number splitting attack for weak coherent state. Such a scheme relies on a smarter encoding scheme that is based on nonorthogonal states and requires at least two or more photons for Eve to recover the data. Thus Eve needs at least three photons to use the photon number splitting attack. If we use this protocol on the modified coherent state, we will make a three-photon interference effect to cancel the three-photon term so that Eve can only rely on the 4-photon or higher order terms to apply the photon number splitting attack. So the modified coherent state still has advantage over a weak coherent state in this new protocol.

Because of the existence of the multi-photon terms, the modified coherent state has similar security problems as the coherent state. But the influence of those higher order terms will be smaller. The security problem of the coherent state was investigated by Lütkenhaus [4] and Brassard et al[17]. In the following, we will apply the same line of argument of Ref.[4] to look for the optimum secure data rate and transmission distance for a given transmission loss and dark counts of the detectors for the modified coherent state in both BB84 protocol in Ref.[3] and the new SARG04 protocol in Ref.[16]. To do that, we need to find the probability P_m for multi-photon event and the probability P_s to detect any photon in such a state. We will start in the following with the description of the modified coherent state.

^{*}currently with Photonics Industries International, Bohemia, NY

[†]Also with Carmel High School, Carmel, IN

[‡]Electronic address: zou@iupui.edu

II. GENERATION OF THE MODIFIED COHERENT STATE (MCS)

The modified coherent state is just a coherent state without the two-photon or three-photon terms. It can be generated by mixing a coherent state with a two-photon state from parametric down-conversion. There are two types of mixing. The first one is to inject the coherent state into an optical parametric amplifier with a small gain. This is the scheme first proposed by Stoler to produce light source with sub-Poissonian statistics. The second one mixes the two fields with a beamsplitter. In practice the first method is more direct and simpler to implement. In the following calculation, the results are more or less same. We will consider only the first method.

For simplicity of argument, we will only treat single mode case here. In reality, this corresponds to, for example, a single temporal mode of pulses of light. We will concentrate on the probabilities of detecting photons in each pulse. The data rate discussed below will be the probability per pulse. In CW case, we will consider the average photon number ($= |\alpha|^2$ for coherent state, see below) rather than the intensity as our parameter. So the detection time does not appear as a separate parameter but is included in the average photon number. However, we do require the detection time be much smaller than the coherence time of the field to ensure the single mode approximation.

In an optical parametric amplifier, the interaction Hamiltonian is given by

$$\hat{H} = j\hbar\xi^* \hat{a}^2/2 + h.c., \quad (1)$$

where ξ is proportional to the amplitude of the pump field and the nonlinear conversion coefficient of the nonlinear medium.

With the injection of a coherent state, the initial state is simply a coherent state $|\alpha\rangle$ and the output state becomes

$$|\Psi\rangle_{out} = \hat{U}|\alpha\rangle \quad (2)$$

with

$$\hat{U} = \exp \frac{1}{2}(\zeta^* \hat{a}^2 - \zeta \hat{a}^{\dagger 2}). \quad (3)$$

ζ is proportional to ξ . As a matter of fact, the above state is simply the two-photon coherent state or the squeezed coherent state first discussed by Yuen[18]. In order to find the probability of photon number, we expand the above state in the photon number state base and obtain from Ref.[18, 19]

$$|\Psi\rangle_{out} = \hat{U}|\alpha\rangle = \sum_{n=0}^{\infty} C_n |n\rangle, \quad (4)$$

with

$$C_n = \frac{1}{\sqrt{n! \mu}} \left(\frac{\nu}{2\mu} \right)^{\frac{n}{2}} \exp \left(\frac{\nu^*}{2\mu} \alpha^2 - \frac{|\alpha|^2}{2} \right) H_n \left(\frac{\alpha}{\sqrt{2\mu\nu}} \right), \quad (5)$$

where H_n is the n th-order Hermite polynomial and

$$\mu \equiv \cosh(|\zeta|), \quad \nu \equiv \frac{\zeta}{|\zeta|} \sinh(|\zeta|), \quad \text{or } \mu^2 = 1 + |\nu|^2.$$

More specifically to our interest, we list

$$\begin{aligned} C_0 &= \frac{1}{\sqrt{\mu}} \exp \left(\frac{\nu^*}{2\mu} \alpha^2 - \frac{1}{2} |\alpha|^2 \right), \\ C_1 &= C_0 \frac{\alpha}{\mu}, \\ C_2 &= \frac{C_0}{\sqrt{2}} \left[-\frac{\nu}{\mu} + \left(\frac{\alpha}{\mu} \right)^2 \right], \\ C_3 &= \frac{C_0}{\sqrt{6}} \left[-\frac{3\nu\alpha}{\mu^2} + \left(\frac{\alpha}{\mu} \right)^3 \right], \\ C_4 &= \frac{C_0}{\sqrt{24}} \left[3 \left(\frac{\nu}{\mu} \right)^2 - 6 \frac{\nu\alpha^2}{\mu^3} + \left(\frac{\alpha}{\mu} \right)^4 \right], \end{aligned}$$

From the above, we easily find the probability for multi-photon event as

$$P_m = 1 - |C_0|^2 - |C_1|^2. \quad (6)$$

This quantity is minimized when

$$\alpha^2 = \mu\nu \quad (7)$$

with a minimum value of

$$P_m = 1 - \frac{1}{\mu} \left(1 + \frac{|\nu|}{\mu} \right) e^{-(\mu - |\nu|)|\nu|}. \quad (8)$$

Notice that the two-photon probability $P_2 = |C_2|^2$ is zero under this condition. This results from a two-photon interference effect between the coherent state and the spontaneous parametric down-conversion, i.e., interference between the two-photon amplitude $\mu\nu/\sqrt{2}$ of parametric down-conversion and the two-photon amplitude $\alpha^2/\sqrt{2}$ of a coherent state.

For SARG04 protocol, we need to minimize the probability for events of three or more photons. This probability is given by

$$P'_m = 1 - |C_0|^2 - |C_1|^2 - |C_2|^2, \quad (9)$$

which is minimized when

$$\alpha^2 = 3\mu\nu \quad (10)$$

with a minimum value of

$$P'_m = 1 - \frac{1}{\mu} \left(1 + \frac{|\nu|}{\mu} \right) \left(1 + \frac{2|\nu|}{\mu} \right) e^{-3(\mu - |\nu|)|\nu|}. \quad (11)$$

Similar to the two-photon case, when condition in Eq.(10) is satisfied, three-photon probability $P_3 = |C_3|^2$ is zero as a result of three-photon interference. It is not easy to understand how a three-photon effect can arise from parametric down-conversion with only even number of photons. What happens is that a two-photon event from parametric down conversion combines with a single photon event in coherent state to form a three-photon

event with an amplitude of $\sqrt{3/2}\mu\nu\alpha$. This amplitude interferes with another three-photon event directly from the coherent state with an amplitude of $\alpha^3/\sqrt{6}$. Complete cancellation occurs when the two amplitudes are equal leading to Eq.(10).

To evaluate the photon detection probability P_s , we notice that in practice, photodetection usually has non-unit efficiency. This will reduce the signal level. We need to calculate the photon detection probability under this non-ideal condition. The non-unit efficiency is modelled as a beamsplitter of transmissivity η . We may start with the photon number probability for single mode case as [19]

$$P_n = \left\langle : \frac{(\hat{a}'^\dagger \hat{a}')^n}{n!} \exp(-\hat{a}'^\dagger \hat{a}') : \right\rangle,$$

where $::$ denotes normal ordering and $\hat{a}' = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{a}_0$ with \hat{a}_0 in the vacuum. More specifically for the case of no photon:

$$P_0 = \langle : \exp(-\hat{a}'^\dagger \hat{a}') : \rangle.$$

Then a simple calculation leads to

$$P_0 = \langle : \exp(-\eta\hat{a}^\dagger \hat{a}) : \rangle, \quad (12)$$

where the average is over the state in Eq.(2). Then the photon detection probability is simply

$$P_s = 1 - P_0. \quad (13)$$

From the appendix, we have

$$P_0 = \frac{\exp\left[-\frac{\eta x^2(\mu-|\nu|)}{\mu+|\nu|(1-\eta)} - \frac{\eta y^2(\mu+|\nu|)}{\mu-|\nu|(1-\eta)}\right]}{\sqrt{\mu^2 - |\nu|^2(1-\eta)^2}} \quad (14)$$

with $x + iy \equiv \alpha e^{-i\varphi/2}$ ($e^{i\varphi} \equiv \nu/|\nu|$).

With the condition in Eq.(7) for minimum multi-photon events, we have the signal probability

$$P_s = 1 - \frac{\exp\left[-\eta\mu|\nu|(\mu-|\nu|)/(\mu+|\nu|(1-\eta))\right]}{\sqrt{\mu^2 - |\nu|^2(1-\eta)^2}}, \quad (15)$$

or

$$P'_s = 1 - \frac{\exp\left[-3\eta\mu|\nu|(\mu-|\nu|)/(\mu+|\nu|(1-\eta))\right]}{\sqrt{\mu^2 - |\nu|^2(1-\eta)^2}} \quad (16)$$

for condition in Eq.(10).

III. OPTIMUM SECURE TRANSMISSION RATE

Next we evaluate the secure transmission rate based on the formulism from Ref.[4]. The communication rate per slot (pulse) for a certain error rate e is given by

$$R = \frac{P_s}{2} \left[\rho(1 - \tau(e)) + f(e)h(e) \right]. \quad (17)$$

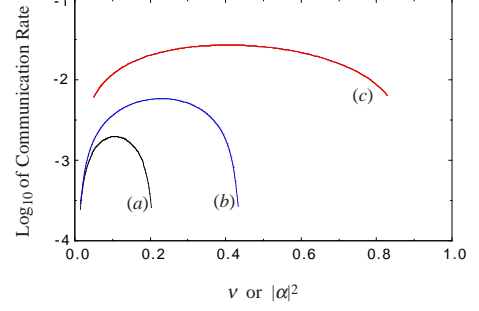


FIG. 1: Communication rate as a function of (a) $|\alpha|^2$ for BB84 with coherent state, (b) ν for BB84 with modified coherent state, and (c) ν for SARG04 with modified coherent state. The overall efficiency is $\eta = -9.45$ dB, which corresponds to a transmission distance of 5 km in KTH15.

In the above equation, the parameter ρ is given by

$$\rho = \frac{P_s - P_m}{P_s}, \quad (18)$$

which is the probability of detection events originating from the desirable photon events. The compression function $\tau(e)$ is given by

$$\tau(e) = \log_2 \left[1 + 4\frac{e}{\rho} - 4\left(\frac{e}{\rho}\right)^2 \right]. \quad (19)$$

The function $h(e)$ is the Shannon entropy function given by

$$h(e) = -e \log_2 e - (1-e) \log_2 (1-e). \quad (20)$$

The function $f(e)$ characterizes the performance of the error correction algorithm.

In order to simulate the communication rate, we need the values of P_s , P_m , e , and $f(e)$. For BB84 protocol with the modified coherent state, P_m and P_s are given in Eqs.(7) and (15), respectively. However, due to the existence of dark count of any photodetectors, Bob's detection events can be contributed from a signal that originates from Alice's transmission, and a dark count that originates from Bob's photodetectors. Therefore, after taking into account the dark counts of the detectors, the signal probability P_s has to be modified as

$$P_s \rightarrow \bar{P}_s = P_s + P_d - P_s P_d, \quad (21)$$

where P_d is the dark count distribution and is simply equal to the dark counts per slot. Similarly, the error rate is also resulted from the signal and the dark count, and can be modelled by

$$e = \frac{cP_s + P_d/2}{\bar{P}_s}, \quad (22)$$

where c is a constant and characterizes a baseline signal error rate. Typical system should have a value of c less

than 2%. The total detection efficiency η can be separated into the channel transmission and the quantum efficiency of Bob's photodetectors. For fiber communications, the transmission in the quantum channel is given by

$$\eta_c = 10^{-(al+L)/10}, \quad (23)$$

where a is the loss coefficient of the fiber channel measured in dB/km, l is the length of the fiber, and L is the loss in the receiver Bob's detection.

We evaluate the communication rate as a function of the free parameters ν ($\mu = \sqrt{1+\nu^2}$) for MCS in BB84 and SARG04 or $|\alpha|^2$ for coherent state, using parameters taken from the case KTH15 in Ref.[4]. The dark counts per slot is $P_d = 2 \times 10^{-4}$. The baseline signal error rate is set to be $c = 0.01$. The loss coefficient a of the fiber channel is 0.2 dB/km, and the receiver loss is 1 dB. The quantum efficiency of the photodetectors is then $\eta = \eta_c \eta_d = 0.18$. The total detection efficiency is then $\eta = \eta_c \eta_d$. For MCS in BB84, P_m and P_s are given in Eqs.(8) and (15) while for SARG04 protocol with MCS, P_m and P_s are from Eqs.(11) and (16), respectively. Fig.1 shows the communication rates as a function of $|\alpha|^2$ at $l = 5$ km for the BB84 protocol with coherent state or as a function of ν for the modified coherent state in BB84 protocol and the SARG04 protocol. As can be seen, there is a clear maximum on the communication rate curve as a function of the adjustable parameter ν or $|\alpha|^2$.

Next we concentrate on the optimal rate as we vary the transmission distance l , then obtain the resulting curves as shown in Fig.2. The overall efficiency η is plotted in the top axis of Fig.2 for reference. The curve (a) is a simple repeat of Ref.[4] for a weak coherent state in BB84. Curves (b) for MCS in BB84 and (c) for MCS in SARG04 have significant improvement over (a). At zero transmission distance, we find a 4 dB increase in secure data rate from modified coherent state over the coherent state in the BB84. A further 6 dB increase in secure data rate is resulted from MCS with SARG04 protocol. Note that each curve features a cutoff transmission distance. Modified coherent state has nearly two-fold increase in transmission distance over the coherent state in BB84. A further nearly two-fold increase in transmission distance is found with SARG04.

Acknowledgments

This paper is based upon work supported by the National Science Foundation under Grant No. 0245421. We wish to acknowledge the support of NSF and the Purdue Research Foundation.

APPENDIX A: CALCULATION OF EQ.(14)

The average in Eq.(12) is over the state in Eq.(4). To do this we first convert Eq.(12) in the normal ordering

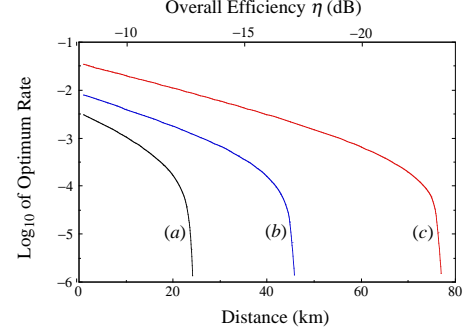


FIG. 2: Optimum rate as a function of transmission distance for: (a) BB84 with coherent state; (b) BB84 with modified coherent state; (c) SARG04 with modified coherent state.

form into one without normal ordering from Ref.[20]:

$$P_0 = \langle : \exp(-\eta \hat{a}^\dagger \hat{a}) : \rangle = \langle \exp[-\ln(1-\eta) \hat{a}^\dagger \hat{a}] \rangle. \quad (A1)$$

Next we convert Eq.(A1) into anti-normal ordering form from Ref.[20] again:

$$\begin{aligned} P_0 &= e^{-\ln(1-\eta)} \langle \mathcal{A}\{\exp[(1-e^{-\ln(1-\eta)})\beta^* \beta]\} \rangle \\ &= \frac{1}{1-\eta} \langle \alpha | \hat{\mathcal{U}}^\dagger \mathcal{A}\{\exp[-\frac{\eta}{1-\eta} \beta^* \beta]\} \hat{\mathcal{U}} | \alpha \rangle. \end{aligned} \quad (A2)$$

Then we insert the closure relation:

$$\frac{1}{\pi} \int d^2 \beta |\beta\rangle \langle \beta| = 1 \quad (A3)$$

between \hat{b}^n and $\hat{b}^{\dagger m}$ in $\mathcal{A}(\beta^* \beta) = \hat{b}^n \hat{b}^{\dagger m}$ in Eq.(A2) and we have

$$P_0 = \frac{1}{\pi} \int d^2 \beta \frac{1}{1-\eta} \exp(-\frac{\eta}{1-\eta} |\beta|^2) |\langle \beta | \hat{\mathcal{U}} | \alpha \rangle|^2. \quad (A4)$$

From Ref.[18, 19] we find

$$\begin{aligned} &\langle \beta | \hat{\mathcal{U}} | \alpha \rangle \\ &= \frac{1}{\sqrt{\mu}} \exp \left[-\frac{|\alpha|^2 + |\beta|^2}{2} + \frac{\nu^* \alpha^2 - \nu \beta^{*2} + 2\beta^* \alpha}{2\mu} \right]. \end{aligned}$$

Substituting the above expression in Eq.(A4) and with some lengthy manipulation, we arrive at the expression in Eq.(14).

-
- [1] W. K. Wootters and W. Zurek, *Nature* **299**, 802 (1982).
[2] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J.

- Smolin, *J. Cryptology* **5**, 3 (1992).
[3] C. H. Bennett and G. Brassard, in *Proceedings of IEEE*

International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp.175-179.

- [4] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
- [5] F. De Martini, G. Di Giuseppe, and M. Marrocco, Phys. Rev. Lett. **76**, 900 (1995).
- [6] S. C. Kitson et al., Phys. Rev. A **58**, 620 (1998).
- [7] C. Brunel et al., Phys. Rev. Lett. **83**, 2722 (1999).
- [8] L. Fleury et al., Phys. Rev. Lett. **84**, 1148 (2000).
- [9] C. Kurtsiefer et al., Phys. Rev. Lett. **85**, 290 (2000).
- [10] R. Brouri et al., Opt. Lett. **25**, 1294 (2000).
- [11] J. Kim et al., Nature **397**, 500 (1999).
- [12] P. Michler et al., Nature **406**, 968 (2000); P. Michler et al., Science **290**, 2282 (2000); C. Santori et al., Phys. Rev. Lett. **86**, 1502 (2001).
- [13] G. S. Solomon, M. Pelton, and Y. Yamamoto, Phys. Rev. Lett. **86**, 3903 (2001).
- [14] A. B. Dodson and Reeta Vyas, Phys. Rev. A **47**, 3396 (1993); H. Deng, D. Erenso, R. Vyas, and S. Singh, Phys. Rev. Lett. **86**, 2770 (2001).
- [15] Y. J. Lu and Z. Y. Ou, Phys. Rev. Lett. **88**, 023601 (2002).
- [16] V. Scacranì, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).
- [17] G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
- [18] H. P. Yuen, Phys. Rev. A **13**, 2226 (1976).
- [19] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, Cambridge University Press, New York (1995).
- [20] W. H. Louisell, *Quantum Statistical Properties of Radiation* (Wiley, New York, 1973), pp.156-159.